The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
05/14/2013

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird applications, which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Firefox versions prior to 21.0
- Firefox Extended Support Release (ESR) versions prior to 17.0.6
- Thunderbird versions prior to 17.0.6
- Thunderbird Extended Support Release (ESR) versions prior to 17.0.6

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird. The details of these vulnerabilities are as follows:

- **Miscellaneous memory safety hazards (MFSA 2013-41) (CVE-2013-0801) (CVE-2013-1669):** Multiple memory-corruption vulnerabilities exist in the browser engine that could lead to arbitrary code execution.
- **Privileged access for content level constructor (MFSA 2013-42) (CVE-2013-1670):** A constructor allows for write actions on objects when only read actions should be allowed. This could lead to cross-site scripting attacks.
- **File input control has access to full path (MFSA 2013-43) (CVE-2013-1671):** This vulnerability is caused by a mechanism that exploits the <input> control when set to a file type in order to get the full path of the file. This can lead to information disclosure and could lead to further attacks in the future.
- **Local privilege escalation through Mozilla Maintenance Service (MFSA 2013-44) (CVE-2013-1672):** This vulnerability allows local unprivileged users to escalate their privileges through the system privileges used by the Mozilla Maintenance Service. Local file system access is necessary for this vulnerability to be exploited.
- **Mozilla Updater fails to update some Windows Registry entries (MFSA 2013-45) (CVE-2013-1673) (CVE-2012-1942):** This vulnerability was caused by the Mozilla Updater not updating Windows Registry entries for the Mozilla Maintenance Service. Therefore, local privilege escalation vulnerabilities that were fixed in previous updates were not being properly applied in some cases.
- **Use-after-free with video and on resize event (MFSA 2013-46) (CVE-2013-1674):** There is a use-after-free vulnerability when resizing video while playing. This could allow for arbitrary code execution.
- **Uninitialized functions in DOMSVGZoomEvent (MFSA 2013-47) (CVE-2013-1675):** A vulnerability was discovered that some DOMSVGZoomEvent functions are used without being properly initialized, causing uninitialized memory to be used when they are called by web content. This could lead to an information leakage to sites depending on the contents of the uninitialized memory.
- **Memory corruption found using Address Sanitizer (MFSA 2013-48) (CVE-2013-1676) (CVE-2013-1677) (CVE-2013-1678) (CVE-2013-1679) (CVE-2013-1680) (CVE-2013-1681):** The Address Sanitizer tool can be used to trigger use-after-free, out of bounds read, and invalid write vulnerabilities. These issues are potentially exploitable and could lead to remote code execution.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:
http://www.mozilla.org/security/announce/
https://www.mozilla.org/security/announce/2013/mfsa2013-41.html
https://www.mozilla.org/security/announce/2013/mfsa2013-42.html
https://www.mozilla.org/security/announce/2013/mfsa2013-43.html
https://www.mozilla.org/security/announce/2013/mfsa2013-44.html
https://www.mozilla.org/security/announce/2013/mfsa2013-45.html
https://www.mozilla.org/security/announce/2013/mfsa2013-46.html
https://www.mozilla.org/security/announce/2013/mfsa2013-47.html
https://www.mozilla.org/security/announce/2013/mfsa2013-48.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0801
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1669
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1670
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1671
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1672
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1673
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1942
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1674
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1675
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1676
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1677
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1678
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1679
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1680
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1681